CS641A End Sem

Punit Chaudhari, Aman Mittal, Piyush Gangle

TOTAL POINTS

35 / 50

QUESTION 1

1 Lattice **10 / 10**

✓ **+ 10 pts** **Correct**

+ 0 pts Incorrect answer or NA

QUESTION 2

2 Decryption **10 / 15**

✓ **+ 15 pts** **Correct**

+ 0 pts Incorrect answer or NA

- 5 **Point adjustment**

1 Not correct

QUESTION 3

3 Cryptosystem Security **15 / 25**

c) Orthogonal basis of $$\hat{L}$$

✓ **+ 15 pts** **Correct**

+ 0 pts Incorrect or NA

d) Other ways of break security

+ 10 pts Correct

+ 0 pts Incorrect or NA

+ 0 pts Incorrect or NA

QUESTION 4

4 References **0 / 0**

✓ **+ 0 pts** **Correct**

CS641

Modern Cryptology

Indian Institute of Technology, Kanpur

Group Name: INSYNC

Aman Mittal (180072), Piyush Gangle (21111046), Punit Chaudhari (21111050)

End Semester Examination

Submission Deadline:
May 5, 2022, 11:55hrs

Solution 1

Lattice

$$\textit{We are given that } L = n.I \tag{1.1}$$

$$\textit{and } \hat{L} = U.L.R \tag{1.2}$$

putting value of L in 1.2 from 1.1, we get,

$$\hat{L} = U.n.I.R \tag{1.3}$$

since A.I = A therefore

$$\hat{L} = n.U.R \tag{1.4}$$

dividing by n on both side we get

$$[\frac{\hat{L}}{n}] = U.R \tag{1.5}$$

taking transpose in we get

$$[(\frac{\hat{L}}{n})^T] = (U.R)^T \tag{1.6}$$

multiplying 1.5 and 1.6 we get

$$\begin{aligned}[\frac{\hat{L}}{n}].[(\frac{\hat{L}}{n})^T] &= (UR)(UR)^T \\ &= U.(R.R^T).U^T\end{aligned}$$

$$\begin{aligned}
since\ R\ is\ orthogonal\ matrix\ thus\ replacing\ (R.R^T)\ by\ I\ we\ get \\
&= (U.I.U^T) \\
&= (U.U^T) \\
since\ U\ is\ an\ unitary\ matrix\ \forall x \in Q^{n*n}\ so\ U\ is\ orthogonal\ U.U^T &= I \\
(\frac{\hat{L}}{n}).(\frac{\hat{L}}{n})^T &= I
\end{aligned}$$

As from the above equation we can see that $A.A^T = I$ so A is orthogonal where $A = (\hat{L}/n)$ which shows that the vectors in this matrix are orthonormal to each other. Also if we multiply n which is a scalar to these vectors they only get scaled up and will remain orthonormal.

As U, L and R are of same size $n \times n$ so $\hat{L}$ will be of size $n \times n$. Therefore, the lattice generated by $\hat{L}$ has a basis consisting of n orthogonal vectors, each of length n.

Alternative Method Using GSO

Now, $\hat{L}$ is not 0, so, it is a non-singular matrix. Coefficients are from $Q \subset \mathbb{R}$.
Now let each of the n basis elements be of length n.

We apply GSO to get the orthogonal basis.
By using the given properties about $L\ and\ \hat{L}$, we conclude that:

$$\det(\hat{L}) = \det(U) \cdot \det(L) \cdot \det(R) = 1 \cdot n.1 \cdot \pm 1 = \pm n$$

As, $\hat{L}$ is an $n \times n$ non-singular matrix. Let, $b_1, b_2, \cdots, b_n$ is the basis of $\hat{L}$. Using Gram-Schmidt Orthogonalization or GSO, we get orthogonal basis. Suppose $\{v_1, v_2, \cdots, v_n\}$ denotes the orthogonal basis computed via GSO each having length n.
So, $\hat{L}$ has basis of n orthogonal vectors each having length n.

Decryption

Proof described below conveys that decryption works correctly.

- For decryption we have to compute

$$d = c * R^t \tag{2.1}$$

- In encryption it is given that vector c,

$$c = (v * \hat{L} + m) \tag{2.2}$$

- Substituting value of c in 2.1

$$d = (v * \hat{L} + m) * R^t \tag{2.3}$$

$$d = v * \hat{L} * R^t + m * R^t \tag{2.4}$$

- Also $\hat{L} = U * L * R$

$$d = v * (U * L * R) * R^t + m * R^t \tag{2.5}$$

1 Lattice 10 / 10

✓ **+ 10 pts** **Correct**

+ 0 pts Incorrect answer or NA

Alternative Method Using GSO

Now, $\hat{L}$ is not 0, so, it is a non-singular matrix. Coefficients are from $Q \subset \mathbb{R}$.
Now let each of the n basis elements be of length n.

We apply GSO to get the orthogonal basis.
By using the given properties about $L\ and\ \hat{L}$, we conclude that:

$$\det(\hat{L}) = \det(U) \cdot \det(L) \cdot \det(R) = 1 \cdot n.1 \cdot \pm 1 = \pm n$$

As, $\hat{L}$ is an $n \times n$ non-singular matrix. Let, $b_1, b_2, \cdots, b_n$ is the basis of $\hat{L}$. Using Gram-Schmidt Orthogonalization or GSO, we get orthogonal basis. Suppose $\{v_1, v_2, \cdots, v_n\}$ denotes the orthogonal basis computed via GSO each having length n.
So, $\hat{L}$ has basis of n orthogonal vectors each having length n.

Decryption

Proof described below conveys that decryption works correctly.

- For decryption we have to compute

$$d = c * R^t \tag{2.1}$$

- In encryption it is given that vector c,

$$c = (v * \hat{L} + m) \tag{2.2}$$

- Substituting value of c in 2.1

$$d = (v * \hat{L} + m) * R^t \tag{2.3}$$

$$d = v * \hat{L} * R^t + m * R^t \tag{2.4}$$

- Also $\hat{L} = U * L * R$

$$d = v * (U * L * R) * R^t + m * R^t \tag{2.5}$$

-Since $R * R^t = I$, and $L = n * I$ so

$$d = v * (U * n * I) + m * R^t \tag{2.6}$$

$$d = n * v * U + m * R^t \tag{2.7}$$

- Taking mod n from the both the sides by following the instruction provided in question

$$d' = (n * v * U + mR^t) modn \tag{2.8}$$

$$d' = (n * v * U) * modn + (m * R^t) modn \tag{2.9}$$

- Therefore $(n * v * U) * modn = 0$ and reducing every entry of $d \mod (n)$, so the entry $|e| < \frac{n}{2}$(Less than n/2)

$$d' = m * R^t \tag{2.10}$$

Now, we perform the decryption:

$$m' = d' * R \tag{2.11}$$

-Putting value of d' from 2.10

$$m' = m * R^t * R \tag{2.12}$$

$$m' = m \tag{2.13}$$

So, since we get back the message, decryption works correctly.

2 Decryption 10 / 15

✓ + **15 pts** **Correct**

+ **0 pts** Incorrect answer or NA

- 5 Point adjustment

1 Not correct

Cryptosystem Security

For Vector v, we know that: $v \in \mathbb{Z}^N$, which means that $v\hat{L}$ exists in an integer lattice vector generated by $\hat{L}$. We know that:

$$c = v\hat{L} + m$$

We now have to find a vector c', such that c-c' = m (Original message)

Let w_k be orthogonal basis vectors of $\hat{L}$. Now, consider the following equation which expresses c in terms of w_k:

$$c = a_k.w_k \quad \ldots \; where \; k = 1 \ldots n$$

Where a_k are all the coefficients. They can be computed by:

$$\langle c, w_i \rangle = \begin{bmatrix} c_1 & c_2 & \ldots & c_n \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ . \\ w_n \end{bmatrix}$$

We are given that $c, w_i \in \mathcal{Q}^N$ So:

$$a_i \in \mathcal{Q}^N.$$

Finally, to compute the coefficients a_i, we use Babai's rounding technique instead of using GSO to get c'. This will approximate the coefficients to their nearest round values and will produce the vector c', which is nearest to c. So:

$$c' = \sum_{k=1}^{n} \lfloor a_k \rceil w_k$$

Now, by taking the difference we get:

$$c - c' = m$$

3 Cryptosystem Security 15 / 25

c) Orthogonal basis of $\hat{L}$

✓ + **15 pts** **Correct**

+ **0 pts** Incorrect or NA

d) Other ways of break security

+ **10 pts** Correct
+ **0 pts** Incorrect or NA

+ **0 pts** Incorrect or NA

References

https://www.math.auckland.ac.nz/ sgal018/crypto-book/ch18.pdf [Page 6]

4 References 0 / 0

✓ + 0 pts Correct